Results for **"((common key, inverse, round function)<in>metadata)"** e-mail
Your search matched **15146** of **1436708** documents.
A maximum of **100** results are displayed, **25** to a page, sorted by **Relevance** in **Descending** order.

1. **Inverse learning based on extension logic**
Bin He; Xiao-Yin Chen; Jing-Guang Gao;
Machine Learning and Cybernetics, 2005. Proceedings of 2005 International C
Volume 5, 18-21 Aug. 2005 Page(s):3042 - 3047 Vol. 5
Digital Object Identifier 10.1109/ICMLC.2005.1527464
AbstractPlus | Full Text: PDF(328 KB) IEEE CNF
Rights and Permissions

2. **A design method for stable delayed-inverse systems for strictly proper di complete diagonalization**
Yamada, K.; Kinoshita, W.; Kikuchi, S.;
Intelligent Control, 2002. Proceedings of the 2002 IEEE International Symposiu
27-30 Oct. 2002 Page(s):907 - 912
Digital Object Identifier 10.1109/ISIC.2002.1157883
AbstractPlus | Full Text: PDF(492 KB) IEEE CNF
Rights and Permissions

3. **New design method for stable filtered inverse systems**
Yamada, K.; Kinoshita, W.;
American Control Conference, 2002. Proceedings of the 2002
Volume 6, 8-10 May 2002 Page(s):4738 - 4743 vol.6
Digital Object Identifier 10.1109/ACC.2002.1025406
AbstractPlus | Full Text: PDF(485 KB) IEEE CNF
Rights and Permissions

4. **Nonlinear hybrid adaptive inverse control using neural fuzzy system and to CSTR systems**
Jia Li; Yu Jinshou;
Intelligent Control and Automation, 2002. Proceedings of the 4th World Congre
Volume 3, 10-14 June 2002 Page(s):1896 - 1900 vol.3
Digital Object Identifier 10.1109/WCICA.2002.1021413
AbstractPlus | Full Text: PDF(497 KB) IEEE CNF
Rights and Permissions

5. **Complexity issues in inverse scattering problems**
Chew, W.C.;
Antennas and Propagation Society International Symposium, 1999. IEEE
Volume 3, 11-16 July 1999 Page(s):1627 vol.3

Digital Object Identifier 10.1109/APS.1999.788258

AbstractPlus | Full Text: PDF(40 KB) IEEE CNF
Rights and Permissions

6. **Effects of experimental and modeling errors on electrocardiographic inve formulations**
Cheng, L.K.; Bodley, J.M.; Pullan, A.J.;
Biomedical Engineering, IEEE Transactions on
Volume 50, Issue 1, Jan. 2003 Page(s):23 - 32
Digital Object Identifier 10.1109/TBME.2002.807325

AbstractPlus | References | Full Text: PDF(641 KB) IEEE JNL
Rights and Permissions

7. **Inverse Jacobian regulator for robot manipulator: theory and experiment**
Cheah, C.C.; Zhao, Y.;
Decision and Control, 2004. CDC. 43rd IEEE Conference on
Volume 2, 14-17 Dec. 2004 Page(s):1252 - 1257 Vol.2

AbstractPlus | Full Text: PDF(1857 KB) IEEE CNF
Rights and Permissions

8. **Towards inverse production life cycle design: a simulation tool linking m recycling to environmental legislation and market**
Jovane, F.; Bosani, R.; Castelli, L.; Salsa, F.;
Environmentally Conscious Design and Inverse Manufacturing, 2001. Proceed 2001: Second International Symposium on
11-15 Dec. 2001 Page(s):924 - 928
Digital Object Identifier 10.1109/.2001.992494

AbstractPlus | Full Text: PDF(519 KB) IEEE CNF
Rights and Permissions

9. **A reconsideration of the pth-order inverse predistorter**
Chi-Hao Cheng; Powers, E.J.;
Vehicular Technology Conference, 1999 IEEE 49th
Volume 2, 16-20 May 1999 Page(s):1501 - 1504 vol.2
Digital Object Identifier 10.1109/VETEC.1999.780597

AbstractPlus | Full Text: PDF(340 KB) IEEE CNF
Rights and Permissions

10. **Initial conditions, sources, and currents for prescribed time-dependent a electromagnetic fields in three dimensions, Part I: The inverse initial valu Acoustic and electromagnetic "bullets," expanding waves, and implodin**
Moses, H.; Prosser, R.;
Antennas and Propagation, IEEE Transactions on [legacy, pre - 1988]
Volume 34, Issue 2, Feb 1986 Page(s):188 - 196

AbstractPlus | Full Text: PDF(840 KB) IEEE JNL
Rights and Permissions

11. **A bioelectric inverse imaging technique based on surface Laplacians**
Bin He; Dongsheng Wu;
Biomedical Engineering, IEEE Transactions on
Volume 44, Issue 7, July 1997 Page(s):529 - 538
Digital Object Identifier 10.1109/10.594893

AbstractPlus | References | Full Text: PDF(256 KB) IEEE JNL
Rights and Permissions

12. **Inverse kinematics learning for robotic arms with fewer degrees of freed neural network systems**
Oyama, E.; Maeda, T.; Gan, J.Q.; Rosales, E.M.; MacDorman, K.F.; Tachi, S.;
Intelligent Robots and Systems, 2005. (IROS 2005). 2005 IEEE/RSJ Internatic

on
2-6 Aug. 2005 Page(s):1791 - 1798
Digital Object Identifier 10.1109/IROS.2005.1545084

AbstractPlus | Full Text: PDF(848 KB) IEEE CNF
Rights and Permissions

☐ **13. Stability of inverse Jacobian control for robot manipulator**
Cheah, C.C.; Liu, C.; Liaw, H.C.;
Control Applications, 2004. Proceedings of the 2004 IEEE International Confe
Volume 1, 2-4 Sept. 2004 Page(s):321 - 326 Vol.1

AbstractPlus | Full Text: PDF(689 KB) IEEE CNF
Rights and Permissions

☐ **14. Inverse kinematics learning by modular architecture neural networks**
Oyama, E.; Tachi, S.;
Neural Networks, 1999. IJCNN '99. International Joint Conference on
Volume 3, 10-16 July 1999 Page(s):2065 - 2070 vol.3
Digital Object Identifier 10.1109/IJCNN.1999.832704

AbstractPlus | Full Text: PDF(432 KB) IEEE CNF
Rights and Permissions

☐ **15. Note on Feedforward Inverses for Linear Sequential Circuits**
Olson, R.R.;
Computers, IEEE Transactions on
Volume C-19, Issue 12, Dec. 1970 Page(s):1216 - 1221

AbstractPlus | Full Text: PDF(1112 KB) IEEE JNL
Rights and Permissions

☐ **16. Minimal Memory Inverses of Linear Sequential Circuits**
Fu-Min Yuan;
Computers, IEEE Transactions on
Volume C-23, Issue 11, Nov. 1974 Page(s):1155 - 1163

AbstractPlus | Full Text: PDF(2568 KB) IEEE JNL
Rights and Permissions

☐ **17. Repeatable generalized inverse control strategies for kinematically redur manipulators**
Roberts, R.G.; Maciejewski, A.A.;
Automatic Control, IEEE Transactions on
Volume 38, Issue 5, May 1993 Page(s):689 - 699
Digital Object Identifier 10.1109/9.277234

AbstractPlus | Full Text: PDF(856 KB) IEEE JNL
Rights and Permissions

☐ **18. Time-varying filters and filter banks: some basic principles**
See-May Phoong; Vaidyanathan, P.P.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Si
IEEE Transactions on]
Volume 44, Issue 12, Dec. 1996 Page(s):2971 - 2987
Digital Object Identifier 10.1109/78.553472

AbstractPlus | References | Full Text: PDF(1768 KB) IEEE JNL
Rights and Permissions

☐ **19. Look-up table (LUT) method for inverse halftoning**
Mese, M.; Vaidyanathan, P.P.;
Image Processing, IEEE Transactions on
Volume 10, Issue 10, Oct. 2001 Page(s):1566 - 1578
Digital Object Identifier 10.1109/83.951541

AbstractPlus | References | Full Text: PDF(672 KB) **IEEE JNL**
Rights and Permissions

☐ **20. Infinite impulse response (IIR) inverse filter design for the equalization of phase loudspeaker systems**
Marques, A.; Freitas, D.;
Applications of Signal Processing to Audio and Acoustics, 2005. IEEE Worksh
16-19 Oct. 2005 Page(s):170 - 173
Digital Object Identifier 10.1109/ASPAA.2005.1540197
AbstractPlus | Full Text: PDF(144 KB) **IEEE CNF**
Rights and Permissions

☐ **21. Inverse kinematics learning by modular architecture neural networks with prediction networks**
Oyama, E.; Nak Young Chong; Agah, A.; Maeda, T.;
Robotics and Automation, 2001. Proceedings 2001 ICRA. IEEE International C
Volume 1, 2001 Page(s):1006 - 1012 vol.1
Digital Object Identifier 10.1109/ROBOT.2001.932681
AbstractPlus | Full Text: PDF(555 KB) **IEEE CNF**
Rights and Permissions

☐ **22. Plasma inverse transition acceleration**
Ming Xie;
Particle Accelerator Conference, 2001. PAC 2001. Proceedings of the 2001
Volume 5, 18-22 June 2001 Page(s):3876 - 3878 vol.5
Digital Object Identifier 10.1109/PAC.2001.988283
AbstractPlus | Full Text: PDF(214 KB) **IEEE CNF**
Rights and Permissions

☐ **23. Inverse distribution system of construction for closed-loop construction**
Nakamura, H.; Shiino, J.;
Environmentally Conscious Design and Inverse Manufacturing, 2001. Proceed
2001: Second International Symposium on
11-15 Dec. 2001 Page(s):696 - 701
Digital Object Identifier 10.1109/.2001.992451
AbstractPlus | Full Text: PDF(1155 KB) **IEEE CNF**
Rights and Permissions

☐ **24. A study of human hand position control learning-output feedback inversi**
Oyama, E.; Maeda, T.; Tachi, S.;
Neural Networks, 1991. 1991 IEEE International Joint Conference on
18-21 Nov. 1991 Page(s):1434 - 1443 vol.2
Digital Object Identifier 10.1109/IJCNN.1991.170601
AbstractPlus | Full Text: PDF(464 KB) **IEEE CNF**
Rights and Permissions

☐ **25. A learning method for solving inverse problems of static systems**
Oyama, E.; Tachi, S.;
Neural Networks, 1993. IJCNN '93-Nagoya. Proceedings of 1993 International on
Volume 3, 25-29 Oct. 1993 Page(s):2843 - 2851 vol.3
Digital Object Identifier 10.1109/IJCNN.1993.714316
AbstractPlus | Full Text: PDF(432 KB) **IEEE CNF**
Rights and Permissions

View: 1-25 | 26-5

Help Contact Us Privacy &

Terms used **common key inverse round function** Found **97,221** of **193,448**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Courses: Exploiting perception in high-fidelity virtual environments
Mashhuda Glencross, Alan G. Chalmers, Ming C. Lin, Miguel A. Otaduy, Diego Gutierrez
July 2006 **Material presented at the ACM SIGGRAPH 2006 conference SIGGRAPH '06**
Publisher: ACM Press
Full text available: pdf(5.25 MB) Additional Information: full citation, abstract

This course introduces high-fidelity virtual environments and explains the key components required to build compelling environments. Then it details perceptually inspired techniques that facilitate high-fidelity rendering, collaboration, and complex interaction in these virtual environments. Particular emphasis is placed on real applications, with several live demonstrations.

2 Courses: An introduction to sketch-based interfaces
Joseph LaViola, Randall Davis, Takeo Igarashi
July 2006 **Material presented at the ACM SIGGRAPH 2006 conference SIGGRAPH '06**
Publisher: ACM Press
Full text available: pdf(31.58 MB) Additional Information: full citation, abstract

Sketch-based interfaces are a natural, pencil-and-paper-like approach to interacting with a variety of applications, including conceptual modeling, animation, and note-taking systems. This course offers an in-depth discussion of sketch-based interface design, ranging from simple gestural commands to complex sketch-understanding systems. Attendees will learn how these interfaces are designed and how to develop their own.

3 The elements of nature: interactive and realistic techniques
Oliver Deusen, David S. Ebert, Ron Fedkiw, F. Kenton Musgrave, Przemyslaw Prusinkiewicz, Doug Roble, Jos Stam, Jerry Tessendorf
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(17.65 MB) Additional Information: full citation, abstract

This updated course on simulating natural phenomena will cover the latest research and production techniques for simulating most of the elements of nature. The presenters will provide movie production, interactive simulation, and research perspectives on the difficult task of photorealistic modeling, rendering, and animation of natural phenomena. The course offers a nice balance of the latest interactive graphics hardware-based simulation techniques and the latest physics-based simulation techni ...

4 Courses: State of the art in interactive ray tracing

Peter Shirley
July 2006 **Material presented at the ACM SIGGRAPH 2006 conference SIGGRAPH '06**
Publisher: ACM Press
Full text available: pdf(14.08 MB) Additional Information: full citation, abstract

Recent improvements in computer hardware have allowed ray tracing to be used in some interactive applications. The trends in architecture and expansions of geometric model should increase the use of interactive ray tracing. This course presents recent and often not-yet published work on interactive ray tracing.

5 The Exact Solution of Linear Equations with Rational Function Coefficients

Michael T. McClellan
March 1977 **ACM Transactions on Mathematical Software (TOMS)**, Volume 3 Issue 1
Publisher: ACM Press
Full text available: pdf(1.58 MB) Additional Information: full citation, references, citings, index terms

6 On randomization in sequential and distributed algorithms

Rajiv Gupta, Scott A. Smolka, Shaji Bhaskar
March 1994 **ACM Computing Surveys (CSUR)**, Volume 26 Issue 1
Publisher: ACM Press
Full text available: pdf(8.01 MB) Additional Information: full citation, abstract, references, citings, index terms

Probabilistic, or randomized, algorithms are fast becoming as commonplace as conventional deterministic algorithms. This survey presents five techniques that have been widely used in the design of randomized algorithms. These techniques are illustrated using 12 randomized algorithms—both sequential and distributed— that span a wide range of applications, including:primality testing (a classical problem in number theory), interactive probabilistic proof s ...

Keywords: Byzantine agreement, CSP, analysis of algorithms, computational complexity, dining philosophers problem, distributed algorithms, graph isomorphism, hashing, interactive probabilistic proof systems, leader election, message routing, nearest-neighbors problem, perfect hashing, primality testing, probabilistic techniques, randomized or probabilistic algorithms, randomized quicksort, sequential algorithms, transitive tournaments, universal hashing

7 Level set and PDE methods for computer graphics

David Breen, Ron Fedkiw, Ken Museth, Stanley Osher, Guillermo Sapiro, Ross Whitaker
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(17.07 MB) Additional Information: full citation, abstract, citings

Level set methods, an important class of partial differential equation (PDE) methods, define dynamic surfaces implicitly as the level set (iso-surface) of a sampled, evolving nD function. The course begins with preparatory material that introduces the concept of using partial differential equations to solve problems in computer graphics, geometric modeling and computer vision. This will include the structure and behavior of several different types of differential equations, e.g. the level set eq ...

8 Magic Functions: In Memoriam: Bernard M. Dwork 1923--1998

Cynthia Dwork, Moni Naor, Omer Reingold, Larry Stockmeyer

November 2003 **Journal of the ACM (JACM)**, Volume 50 Issue 6
Publisher: ACM Press

Full text available: pdf(708.05 KB) Additional Information: full citation, abstract, references, citings, index terms

We prove that three apparently unrelated fundamental problems in distributed computing, cryptography, and complexity theory, are essentially the same problem. These three problems and brief descriptions of them follow. (1) *The selective decommitment problem.* An adversary is given commitments to a collection of messages, and the adversary can ask for some subset of the commitments to be opened. The question is whether seeing the decommitments to these open plaintexts allows the adversary t ...

Keywords: Digital signature, Fiat-Shamir methodology, interactive argument, interactive proof system, magic function, selective decommitment, zero knowledge

9 GPGPU: general purpose computation on graphics hardware

David Luebke, Mark Harris, Jens Krüger, Tim Purcell, Naga Govindaraju, Ian Buck, Cliff Woolley, Aaron Lefohn
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press

Full text available: pdf(63.03 MB) Additional Information: full citation, abstract, citings

The graphics processor (GPU) on today's commodity video cards has evolved into an extremely powerful and flexible processor. The latest graphics architectures provide tremendous memory bandwidth and computational horsepower, with fully programmable vertex and pixel processing units that support vector operations up to full IEEE floating point precision. High level languages have emerged for graphics hardware, making this computational power accessible. Architecturally, GPUs are highly parallel s ...

10 Special section: Reasoning about structure, behavior and function

B. Chandrasekaran, Rob Milne
July 1985 **ACM SIGART Bulletin**, Issue 93
Publisher: ACM Press

Full text available: pdf(5.13 MB) Additional Information: full citation, abstract, references

The last several years' of work in the area of knowledge-based systems has resulted in a deeper understanding of the potentials of the current generation of ideas, but more importantly, also about their limitations and the need for research both in a broader framework as well as in new directions. The following ideas seem to us to be worthy of note in this connection.

11 Universal one-way hash functions and their cryptographic applications

M. Naor, M. Yung
February 1989 **Proceedings of the twenty-first annual ACM symposium on Theory of computing**
Publisher: ACM Press

Full text available: pdf(1.15 MB) Additional Information: full citation, abstract, references, citings, index terms

We define a Universal One-Way Hash Function family, a new primitive which enables the compression of elements in the function domain. The main property of this primitive is that given an element x. We prove constructively that universal one-way hash functions exist if any 1-1 one-way functions exist. Among the various applications of the primitive is a One-Way based Secure Digital Signature Scheme, a system which is based on the ...

12 An asynchronous protocol for distributed computation of RSA inverses and its

applications
Christian Cachin
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing**
Publisher: ACM Press
Full text available: pdf(1.19 MB) Additional Information: full citation, abstract, references, index terms

This paper presents an efficient asynchronous protocol to compute RSA inverses with respect to a public RSA modulus *N* whose factorization is secret and shared among a group of parties. Given two numbers x and e, the protocol computes *y* such that $y^e \equiv x \pmod{N}$. A synchronous protocol for this task has been presented by Catalano, Gennaro, and Halevi (Eurocrypt 2000), but the standard approach for turning this into an asynchronous protocol would re ...

Keywords: Byzantine agreement, Cryptography, threshold signatures, verifiable random functions, verifiable secret sharing

13 Authenticated group key agreement and friends
Giuseppe Ateniese, Michael Steiner, Gene Tsudik
November 1998 **Proceedings of the 5th ACM conference on Computer and communications security**
Publisher: ACM Press
Full text available: pdf(1.05 MB) Additional Information: full citation, references, citings, index terms

14 Computing curricula 2001
September 2001 **Journal on Educational Resources in Computing (JERIC)**
Publisher: ACM Press
Full text available: pdf(613.63 KB) html(2.78 KB) Additional Information: full citation, references, citings, index terms

15 Revised report on the algorithmic language scheme
H. Abelson, R. K. Dybvig, C. T. Haynes, G. J. Rozas, N. I. Adams, D. P. Friedman, E. Kohlbecker, G. L. Steele, D. H. Bartley, R. Halstead, D. Oxley, G. J. Sussman, G. Brooks, C. Hanson, K. M. Pitman, M. Wand
July 1991 **ACM SIGPLAN Lisp Pointers**, Volume IV Issue 3
Publisher: ACM Press
Full text available: pdf(4.08 MB) Additional Information: full citation, abstract, citings, index terms

The report gives a defining description of the programming language Scheme. Scheme is a statically scoped and properly tail-recursive dialect of the Lisp programming language invented by Guy Lewis Steele Jr. and Gerald Jay Sussman. It was designed to have an exceptionally clear and simple semantics and few different ways to form expressions. A wide variety of programming paradigms, including imperative, functional, and message passing styles, find convenient expression in Scheme.

16 Link and channel measurement: A simple mechanism for capturing and replaying wireless channels
Glenn Judd, Peter Steenkiste
August 2005 **Proceeding of the 2005 ACM SIGCOMM workshop on Experimental approaches to wireless network design and analysis E-WIND '05**
Publisher: ACM Press

Full text available: pdf(6.06 MB) Additional Information: full citation, abstract, references, index terms

Physical layer wireless network emulation has the potential to be a powerful experimental tool. An important challenge in physical emulation, and traditional simulation, is to accurately model the wireless channel. In this paper we examine the possibility of using on-card signal strength measurements to capture wireless channel traces. A key advantage of this approach is the simplicity and ubiquity with which these measurements can be obtained since virtually all wireless devices provide the req ...

Keywords: channel capture, emulation, wireless

17 Concurrent zero-knowledge

Cynthia Dwork, Moni Naor, Amit Sahai
November 2004 **Journal of the ACM (JACM)**, Volume 51 Issue 6
Publisher: ACM Press
Full text available: pdf(316.80 KB) Additional Information: full citation, abstract, references, index terms

Concurrent executions of a zero-knowledge protocol by a single prover (with one or more verifiers) may leak information and may not be zero-knowledge *in toto*. In this article, we study the problem of maintaining zero-knowledge.We introduce the notion of an (α, β) *timing constraint*: for any two processors P_1 and P_2, if P_1 measures α elapsed time on its local clock and P_2 measures β elapsed ...

Keywords: Zero knowledge, composition, cryptographic protocols

18 Real-time shading

Marc Olano, Kurt Akeley, John C. Hart, Wolfgang Heidrich, Michael McCool, Jason L. Mitchell, Randi Rost
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(7.39 MB) Additional Information: full citation, abstract

Real-time procedural shading was once seen as a distant dream. When the first version of this course was offered four years ago, real-time shading was possible, but only with one-of-a-kind hardware or by combining the effects of tens to hundreds of rendering passes. Today, almost every new computer comes with graphics hardware capable of interactively executing shaders of thousands to tens of thousands of instructions. This course has been redesigned to address today's real-time shading capabili ...

19 Shape-based retrieval and analysis of 3D models

Thomas Funkhouser, Michael Kazhdan
August 2004 **ACM SIGGRAPH 2004 Course Notes SIGGRAPH '04**
Publisher: ACM Press
Full text available: pdf(12.56 MB) Additional Information: full citation, abstract

Large repositories of 3D data are rapidly becoming available in several fields, including mechanical CAD, molecular biology, and computer graphics. As the number of 3D models grows, there is an increasing need for computer algorithms to help people find the interesting ones and discover relationships between them. Unfortunately, traditional text-based search techniques are not always effective for 3D models, especially when queries are geometric in nature (e.g., find me objects that fit into thi ...

20 Robust efficient distributed RSA-key generation

Yair Frankel, Philip D. MacKenzie, Moti Yung

May 1998 **Proceedings of the thirtieth annual ACM symposium on Theory of computing**
Publisher: ACM Press
Full text available: pdf(1.47 MB) Additional Information: full citation, references, citings, index terms

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used **expanded key** Found **12** of **193,448**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 12 of 12

Relevance scale

1 Survey and benchmark of block ciphers for wireless sensor networks
Yee Wei Law, Jeroen Doumen, Pieter Hartel
February 2006 **ACM Transactions on Sensor Networks (TOSN)**, Volume 2 Issue 1
Publisher: ACM Press
Full text available: pdf(354.39 KB) Additional Information: full citation, abstract, references, index terms

Cryptographic algorithms play an important role in the security architecture of wireless sensor networks (WSNs). Choosing the most storage- and energy-efficient block cipher is essential, due to the facts that these networks are meant to operate without human intervention for a long period of time with little energy supply, and that available storage is scarce on these sensor nodes. However, to our knowledge, no systematic work has been done in this area so far. We construct an evaluation framew ...

Keywords: Sensor networks, block ciphers, cryptography, energy efficiency

2 VIA PadLock-wicked fast encryption
Michal Ludvig
May 2005 **Linux Journal**, Volume 2005 Issue 133
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(24.00 KB) Additional Information: full citation, abstract, index terms

Add hardware support for a common task and measure the performance improvements.

3 Protocol design for scalable and reliable group rekeying
X. Brian Zhang, Simon S. Lam, Dong-Young Lee, Y. Richard Yang
December 2003 **IEEE/ACM Transactions on Networking (TON)**, Volume 11 Issue 6
Publisher: IEEE Press
Full text available: pdf(982.86 KB) Additional Information: full citation, abstract, references, citings, index terms

We present the design and specification of a protocol for scalable and reliable group rekeying together with performance evaluation results. The protocol is based upon the use of key trees for secure groups and periodic batch rekeying. At the beginning of each rekey interval, the key server sends a rekey message to all users consisting of encrypted new keys (encryptions, in short) carried in a sequence of packets. We present a scheme for identifying keys, encryptions, and users, and a key assign ...

Keywords: adaptive FEC, group key management, proactive FEC, reliable multicast, secure multicast

4 An Efficient Hierarchical Timing-Driven Steiner Tree Algorithm for Global Routing
Jingyu Xu, Xianlong Hong, Tong Jing, Yici Cai, Jun Gu
January 2002 **Proceedings of the 2002 conference on Asia South Pacific design automation/VLSI Design**
Publisher: IEEE Computer Society
Full text available: pdf(1.12 MB) Additional Information: full citation, abstract, citings
Publisher Site

In this paper, we propose a hierarchical timing-driven Steiner tree algorithm for global routing which considers the minimization of timing delay during the tree construction as the goal. The algorithm uses heuristic approach to decompose the problem of minimum delay Steiner tree into hierarchy and to construct the sub-trees respectively based on dynamic programming technique. Taking the net topology into consideration, we build the final routing tree by reconnecting the sub-trees at each level ...

5 DIALOG: An operational on-line reference retrieval system
Roger K. Summit
January 1967 **Proceedings of the 1967 22nd national conference**
Publisher: ACM Press
Full text available: pdf(581.55 KB) Additional Information: full citation, abstract, references, citings, index terms

Classification systems in the sciences usually provide an unambiguous structure of mutually exclusive, collectively exhaustive categories. The same formal structuralization, when strictly applied to the classification of technical literature for retrieval purposes, has proved inadequate. At another extreme, approaches to indexing which preclude any hierarchical association are similarly disappointing.

6 IP Easy-pass: a light-weight network-edge resource access control
Haining Wang, Abhijit Bose, Mohamed El-Gendy, Kang G. Shin
December 2005 **IEEE/ACM Transactions on Networking (TON)**, Volume 13 Issue 6
Publisher: IEEE Press
Full text available: pdf(721.97 KB) Additional Information: full citation, abstract, references, index terms

Providing real-time communication services to multimedia applications and subscription-based Internet access often requires that sufficient network resources be reserved for real-time traffic. However, the reserved network resource is susceptible to resource theft and abuse. Without a resource access control mechanism that can efficiently differentiate legitimate real-time traffic from attacking packets, the traffic conditioning and policing enforced at Internet Service Provider (ISP) edge route ...

Keywords: network QoS, resource access control

7 The Mesa programming environment
Richard E. Sweet
June 1983 **ACM SIGPLAN Notices , ACM SIGPLAN Notices , Proceedings of the ACM SIGPLAN 85 symposium on Language issues in programming environments**, Volume 18 , 20 Issue 6 , 7
Publisher: ACM Press
Full text available: pdf(1.48 MB) Additional Information: full citation, abstract, references, index terms

People everywhere are developing multi-window, integrated programming environments for their favorite computers and languages. This paper describes the Mesa programming facilities of the Xerox Development Environment (XDE). It is interesting for several reasons. It has existed in something similar to its current form for about 5 years. It has more than 500 users, many interacting with it 8 or more hours a day. Several million lines of code have been written by these users, including large, ...

8 Ranking text units according to textual saliency, connectivity and topic aptness

Antonio Sanfilippo

August 1998 **Proceedings of the 17th international conference on Computational linguistics - Volume 2 , Proceedings of the 36th annual meeting on Association for Computational Linguistics - Volume 2**

Publisher: Association for Computational Linguistics , Association for Computational Linguistics

Full text available: pdf(586.85 KB) Publisher Site Additional Information: full citation, abstract, references

An efficient use of lexical cohesion is described for ranking text units according to their contribution in defining the meaning of a text (textual saliency), their ability to form a cohesive subtext (textual connectivity) and the extent and effectiveness to which they address the different topics which characterize the subject matter of the text (topic aptness). A specific application is also discussed where the method described is employed to build the indexing component of a summarization sys ...

9 Embedded systems: applications, solutions and techniques (EMBS): Efficient AES implementations for ARM based platforms

Kubilay Atasu, Luca Breveglieri, Marco Macchetti

March 2004 **Proceedings of the 2004 ACM symposium on Applied computing**

Publisher: ACM Press

Full text available: pdf(147.45 KB) Additional Information: full citation, abstract, references

The Advanced Encryption Standard (AES) contest, started by the U.S. National Institute of Standards and Technology (NIST), saw the Rijndael [13] algorithm as its winner [11]. Although the AES is fully defined in terms of functionality, it requires best exploitation of architectural parameters in order to reach the optimum performance on specific architectures. Our work concentrates on ARM cores [1] widely used in the embedded industry. Most promising implementation choices for the common ARM Ins ...

Keywords: AES, ARM microprocessor, cache memories, code optimisation

10 Power modeling and optimization for embedded systems: Analyzing the energy consumption of security protocols

Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha

August 2003 **Proceedings of the 2003 international symposium on Low power electronics and design**

Publisher: ACM Press

Full text available: pdf(271.69 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is critical to a wide range of wireless data applications and services. While several security mechanisms and protocols have been developed in the context of the wired Internet, many new challenges arise due to the unique characteristics of battery powered embedded systems. In this work, we focus on an important constraint of such devices -- battery life -- and examine how it is impacted by the use of security protocols.We present a comprehensive analysis of the energy requirements of a ...

Keywords: 3DES, AES, DES, DSA, Diffie-Hellman, ECC, RSA, SSL, cryptographic algorithms, embedded system, energy analysis, handheld, low-power, security, security protocols

11 Preparing a presentation

Martin Smith
April 1990 **ACM SIGCHI Bulletin**, Volume 21 Issue 4
Publisher: ACM Press
Full text available: pdf(248.93 KB) Additional Information: full citation, abstract, index terms

You are developing a Human Factors curriculum and you have dictatorial control. What will you do? I myself might count on the CHI Curriculum Committee to produce something soon enough to help structure the course content, and focus my attention elsewhere. For example, I would require that each term, students use a different computer system and a different set of applications to write programs and papers, run experiments, analyze data, record notes, etc. At the end of each term they are to delive ...

12 Rooms: the use of multiple virtual workspaces to reduce space contention in a window-based graphical user interface

D. Austin Henderson, Stuart Card
July 1986 **ACM Transactions on Graphics (TOG)**, Volume 5 Issue 3
Publisher: ACM Press
Full text available: pdf(4.58 MB) Additional Information: full citation, abstract, references, citings, index terms

A key constraint on the effectiveness of window-based human-computer interfaces is that the display screen is too small for many applications. This results in "window thrashing," in which the user must expend considerable effort to keep desired windows visible. Rooms is a window manager that overcomes small screen size by exploiting the statistics of window access, dividing the user's workspace into a suite of virtual workspaces with transitions among them. Mech ...

Results 1 - 12 of 12